



UNITED STATES MARINE CORPS

MARINE CORPS BASE
QUANTICO, VIRGINIA 22134-5001

MCBO 2231.1
C 20/k
16 Apr 92

MARINE CORPS BASE ORDER 2231.1

From: Commanding General
To: Distribution List

Subj: SECURE TELEPHONE UNIT - III SOP

Ref: (a) MCO 2231.3
(b) STU-III Key Management Plan EKMS-702.01 (NOTAL)
(c) NTISSI No. 3013 of 8 Feb 90 (NOTAL)
(d) CMS-6 (NOTAL)

1. Purpose. To promulgate the SOP for the management of Secure Telephone Unit - III (STU-III) assets aboard this Command.

2. Cancellation. MCCDCO 2231.1.

3. Summary of Revision. The procedures for STU-III maintenance are now included in paragraph 11. Action for the Commander, Marine Corps Systems Command has been deleted from paragraph 15.

4. Information

a. Amplifying guidance for STU-III key and terminal management is provided in the references.

b. The STU-III was designed as a modern desk top device capable of operating in the secure voice and data mode in an administrative office. The STU-III terminal is designed to protect sensitive/classified information at all levels up to Top Secret Sensitive Compartmented Information (SCI). STU-III's are identified as nontactical, secure voice terminals and are to be installed and maintained by the station telephone personnel.

c. STU-III Communication Security (COMSEC) material is distributed through the Communications Security Material System (CMS) to registered STU-III COMSEC Accounts.

(1) The Department of the Navy (DON) Central Office of Record (COR) provides accountability controls for STU-III terminals.

(2) The National Security Agency's (NSA's) National Central Accounting Office provides accountability controls for STU-III Key Encryption Keying (KEK) material through the STU-III Key Management System (KMS).

MCBO 2231.1
16 Apr 92

d. The procedures in this Order apply only to STU-III COMSEC equipment and associated **KEK's**, and not to any other COMSEC material held by traditional CMS accounts.

e. All STU-III COMSEC material must be stored and protected per OPNAVINST 5510.1 for the level of classification of the material. Additional security requirements are required to limit access to **KEK's** and master Crypto-Ignition Keys (**CIK's**) per paragraph 6 of this Order.

f. Unkeyed STU-III terminals are unclassified, but must be afforded protection as high value Government property. However, when a terminal is keyed, it assumes the classification of the key loaded into it and must be provided physical security at that level.

g. Proper control of COMSEC material is ensured by issuing material only to the appropriate registered STU-III COMSEC Accounts (**SCA's**). Each SCA must contain at least 100 STU-III terminals. The SCA provides security, handling, and accountability controls for STU-III equipment and **KEK's**. SCA custodians are guided by the procedures outlined in references (b) and (c), and STU-III Information Bulletins published by the Commandant of the Marine Corps (CMC). Reference (d) will become the guide when it is formally published.

5. Definitions. For the purpose of this Order, the following definitions apply:

a. Key Storage Device (KSD). The name given to the physical device that can be used as a fill-device and also as a **CIK** for all STU-III's. It is a small device shaped like a physical key and contains passive memory. When it is used to carry a key to a STU-III, it is called a fill device; and when used as a protect key that has been loaded into a STU-III, it is called a **CIK**.

b. Crypto-Ignition Key (CIK). A KSD that contains information used to electronically lock and unlock a STU-III's secure mode. The secure mode is unlocked when the **CIK** is inserted and locked when it is removed.

c. Master Crypto-Ignition Key (CIK). The first **CIK** created for a STU-III, which has been designated to allow the SCA custodian to create additional **CIK's** whenever they are required, up to the STU-III's maximum of eight.

d. Keyed STU-III. A STU-III which has been keyed and in which any of its associated **CIK's** is inserted.

e. Unkeyed STU-III. A STU-III which contains no **CIK** inserted.

f. Key Encryption Key (KEK). A key used in the encryption and/or decryption of other keys for transmission or storage.

g. Seed Key Encryption Key (KEK). Contains the authentication information and only permits call to the KMS. KMS electronically provides an operational KEK to replace the seed KEK. Once this process, called "conversion" is complete, the STU-III may be used in the secure mode.

h. Operational Key Encryption Key (KEK). Contains the authentication information and once loaded into a STU-III it is fully operational and secure calls can be placed.

6. STU-III Security Requirements

a. Operational KEK. Operational KEK's will be afforded protection commensurate with the classification indicated on the Fill Device (FD) label. An Operational KEK must be maintained under Two-Person Integrity (TPI).

b. Seed KEK. Seed KEK's will be afforded protection commensurate with the classification of the key to which it will be converted. TPI does not apply.

c. Master CIK's. The master CIK will be the subject of additional controls to prevent its loss or use to make unauthorized CIK's or unauthorized secure calls. Storage of the master CIK will be commensurate with the classification of the KEK with which they are associated. TPI does not apply.

d. CIK's. CIK's should normally be retained by authorized persons, who should protect them as valuable personal property. Any person who is permitted unrestricted access to the keyed terminal will retain the CIK in their personal possession; i.e., on personal house/car key chain. If stored in the same room as the terminal, the CIK must be afforded protection commensurate with the classification of the keyed terminal (e.g., in an approved security container). The CIK could also be stored in an area apart from the terminal under the best conditions available (e.g., a locked cabinet may be sufficient).

e. Unkeyed STU-III's. Unkeyed STU-III's are unclassified. They will be provided security as a high value item.

f. Keyed STU-III's. Keyed STU-III's will be provided security at the classification level of the KEK used to load it.

g. Audio Security. Audio security should be ruled by common sense. Audio security requirements should not be made so restrictive as to defeat the purpose of having a readily available secure voice system.

h. Command Emergency Action Plan (EAP). Per reference (b), STU-III's must be incorporated into the EAP. The EAP must consider and itemize all tasks necessary to load/destroy all STU-III keying

MCBO 2231.1
16 Apr 92

material, zeroized all loaded terminals, and to account for material being destroyed WHICH IS SECOND IN IMPORTANCE ONLY TO THE DESTRUCTION ITSELF.

i. Zeroizing Procedures. Reference (c) provides zeroizing procedures for STU-III telephones.

7. Personnel Requirements

a. Each SCA must have one custodian meeting the following requirements:

(1) U.S. citizen.

(2) Commissioned officer, enlisted person grade E-6 or above, or civilian government employee GS-7 or above, all of which have a minimum of six months government service.

(3) Possess a security clearance equal to or higher than the highest classification of material to be held by the account. Clearances must also be equal to or higher than the classification to which seed KEK can be converted or operational KEK held.

(4) There is no restriction on serving consecutive tours as an SCA custodian. This applies to SCA custodians, SCA custodians who later become CMS custodians, and CMS custodians who later become SCA custodians.

b. Each SCA must have at least one alternate custodian. Additional alternate custodians may be assigned as required to meet operational requirements. They must meet the same requirements as the custodian.

c. Personnel currently serving as a CMS custodian or primary alternate may not simultaneously serve as the custodian or alternate in an SCA account.

8. Managing STU-III Terminals

a. Responsibility. The equipment SCA, managed by the Director, Data/Communications Integration Division (D/CID), is responsible for installation, repair, and maintenance of all terminals at Marine Corps Combat Development Command (MCCDC). Any movement of STU-III's between users or between a user and another account, including returns to vendors for repair, must be executed by the custodian of the equipment SCA. Increases or decreases of terminal holdings will be handled by the equipment SCA custodian.

b. Local Custody of Terminals. STU-III's will be issued to the unit/organization's supply for induction into the supply (Property Accountability) system. This issue will be based on the STU-III authorized distribution list. The equipment SCA custodian will make this issue on a SF-153.

c. Property Control of Terminals. The unit/organization supply officer will add the STU-III terminals to the Mechanized Allowance List (MAL), Part 2, and the respective Consolidated Memorandum Receipts (CMR's) accordingly. The unit/organizational supply officer will provide a serialized inventory to the Director, Logistics Division upon request. This information will be used for the annual terminal inventory supplied by, reported to and reconciled with the Director, Communications Security Materiel Systems (DCMS). The terminals will be added by serial number, utilizing local NSN's and TAM's listed below:

<u>TAM #</u>	<u>NSN</u>	<u>NOMENCLATURE</u>
HL060	5805-01-Q00-C626	STU-III C2W/MOTOROLA
	5805-01-Q00-C627	STU-III CMK/MOTOROLA
	5805-01-Q00-D829	STU-III CELLULAR
	5805-01-Q00-D830	STU-III CMK/AT&T
	5805-01-Q00-D831	STU-III C2W/AT&T
	5805-01-Q00-D832	STU-III C2W/RCA
	5805-01-Q00-D833	STU-III CMK/RCA

Note: C2W=Single Line CMK=Multi-line

9. Managing STU-III Keying Material

a. The keying material SCA custodian is responsible for all facets of key management. All KEK requests (receipts, transfers, destructions, STU-III KEK loading, and creation of CIK's) must be performed by the keying material SCA custodian or alternate only.

b. STU-III operational and seed KEK's are accountable to the KMS by serial number from receipt by an account until destruction or transfer to another account.

c. Seed and operational KEK's are considered destroyed for accountability purposes once the terminal has been successfully keyed and a CIK has been created. Operational KEK's must be reported to KMS with a destruction report. Seed KEK's do not require a destruction report since they are automatically dropped after the call to the KMS.

d. Increases and decreases of KEK holdings must be executed by the Keying Material SCA Custodian or alternate.

e. Local custody of keying material STU-III KEK's and master CIK's are not authorized for local custody issue to users. The custodian or alternate only must retain possession of STU-III KEK's and master CIK's at all times. Only the custodian or alternate is authorized to load key into a STU-III or create additional user CIK's with a master CIK.

f. Keymat inventories are supplied by, reported to, and reconciled with the KMS. Information copies of keymat inventories are forwarded to DCMS.

MCBO 2231.1
16 Apr 92

10. Manasins Keyed Terminals and CIK's

a. Office Environment. In an office environment where the same people always work together, CIK's will be issued to individual users. The CIK's may stay with the user and be taken home at night or locked in a safe that provides secure storage to the level of the associated keyed terminal.

b. Watch Stations. In an environment where different groups of people rotate in and out of the same office, CIK's will be issued to a position or location, i.e., the watch supervisor position, and they will be inventoried and accounted for on a watch-to-watch basis.

11. STU-III Maintenance Procedures. STU-III terminals that need repair must be returned to the STU-III Custodian for return to the repair facility. The terminals should be turned in to building 1999 (Telephone Office). Please call extension 2500 to coordinate the turn-in. The custodian will require the following information:

a. Probable cause of the problem.

b. STU-III terminal with the following items:

(1) Handset with cord

(2) Power Supply with cord

(3) Box, if available

c. Marine Air-Ground Training and Education Center (MAGTEC); Marine Corps Systems Command (MARCORSYSCOM) . Marine Corps Operational Testing and Evaluation Activity (MCOTEA); USMC Intelligence Center (Intel Ctr); Marine Security Guard Battalion (MSGBn), and Naval Medical Clinic (NMCL) need to provide a funded delivery order (i.e., GSA Form 300, DD Form 1155 or equivalent) for the amount needed for repairs. List the serial number of the phone(s) and part number 5DGA97A (Motorola, \$640) or 5DGA96A (GSA Contract GS-00K-91AFD2269, \$595). Make delivery order to the following:

Motorola, Incorporated
3332 East Broadway Road
Suite 202
Phoenix, AZ 85040-2830

d. In all cases the STU-III terminal will be returned to the unit after repairs have been made.

12. Requesting STU-III Telephones and KEK's

a. Telephones. STU-III telephones will be issued by the unit/organization's supply. Requests for installation are made by

submitting a Telephone Work Request through proper channels to the Director, D/CID (C 201).

b. KEK's. Keying material is requested by submitting a memorandum to the Commanding General, MCCDC (C 013) with the following information:

- (1) Serial number of STU-III telephone.
- (2) Location of STU-III telephone.
- (3) Name of individual(s) who will be using the telephone with their security accesses.
- (4) STU-III telephone number.
- (5) Classification of KEK to be ordered for particular STU-III.
- (6) Authentication information required for STU-III.

c. Due to security and technical considerations all requests to connect a STU-III to a facsimile, modem, or computer terminal will be sent to the Commanding General, MCCDC (C 20).

13. Reportable Insecurities. The following events must be reported to the Commanding General, MCCDC (C 013) immediately by the user.

a. Any instance where the authentication information displayed during a secure call is not representative of the organization in which the distant terminal is located.

b. Any instance where the display indicates that the distant terminals' key has been compromised.

c. Any instance where material is left unattended, improperly stored, or material is destroyed using improper methods.

d. Any instance where there is loss of material. If the record of destruction or transfer cannot be located, then the material should be reported as lost.

e. Any instance where material is found outside of required accountability (for example, material reported as destroyed is found partially or wholly intact).

f. Any instance where packages of material received are improperly packaged, damaged, or show evidence of tampering.

g. Any instance where individuals possessing detailed knowledge of STU-III equipment or other COMSEC material are reported in an unauthorized absence status.

MCBO 2231.1
16 Apr 92

14. Insecure Practices

a. All STU-III users must report insecure practices as soon as **possible** after they occur to the Commanding General, MCCDC (C 013). These insecure practices are particularly germane to the STU-III terminal and its key:

(1) The loss of any CIK.

(2) Failure to rekey a terminal within 60 days of the **key's** expiration date.

(3) Transmission of classified information using a terminal whose display has failed.

(4) Failure to protect adequately or to zeroize a CIK that is associated with a lost terminal.

b. Unless there is an indication of espionage or sabotage, insure practices are not reported outside of MCCDC.

c. Command action will be taken, however, to monitor and evaluate insecure practices for accessing corrective **followup** action.

15. Action

a. Director, Data/Communications Intesration Division. Establish an equipment SCA to support MCCDC and all tenant activities.


b. Command Adjutant. Establish a Key Material SCA to support MCCDC and tenant activities.

c. Director, Logistics Division

(1) Ensure all accountable supply officers of MCCDC maintain the STU-III terminals **on Part 2 of the units' MAL if an allowance is** required.

(2) Provide the Director, D/CID a serialized inventory of STU-III terminals upon request or at least annually.

d. Commander, Marine Corps Systems Command. Establish a keying material SCA to support MARCORSYSCOM elements at MCCDC.


T. C. TAYLOR
By direction

DISTRIBUTION: A